IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK USER ID DONTE KANE THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK INC.	Case No. 19-0329 BPG
IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH INSTAGRAM USER ID DONTE KANE666 THAT IS STORED AT PREMISES CONTROLLED BY INSTAGRAM, LLC	Case No. 19-0330 BPG

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Mohammed Ali, a Detective with the Baltimore Police Department and a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI") being duly sworn, states:

INTRODUCTION AND AGENT BACKGROUND

1. I am currently investigating a string of armed robberies occurring in Baltimore City and Baltimore and Anne Arundel Counties. The investigation involves at least three known and unknown targets, including Donte DINGLE a/k/a Donte Kane who is the primary suspect under investigation.

2. I make this affidavit in support of an application for a search warrant for the following accounts (collectively referred to as the "**Target Accounts**") believed to be used by DINGLE:

a. Information associated with Facebook user ID "Donte Kane" (Facebook ID: Donte.Kane) that is stored at premises owned, maintained, controlled, or operated by

Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California.

b. Information associated with Instagram user ID "Donte Kane666" (Instagram ID: dontekane) that is stored at premises owned, maintained, controlled, or operated by Instagram, LLC ("Instagram"), a social-networking company owned by Facebook, Inc. and headquartered in San Francisco, California.

3. Based on my training and experiences and the facts as set forth in this affidavit, there is probable cause to believe that DINGLE has committed criminal offenses, to wit, Hobbs Act robbery and conspiracy to commit Hobbs Act Robbery in violation of 18 U.S.C. § 1951, felon in possession of a firearm in violation of 18 U.S.C. § 922(g), and use of a firearm in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c) (collectively referred to as the "**Target Offenses**"). There is also probable cause to search the **Target Accounts** for information described in Attachments A-1 and A-2 for evidence of the **Target Offenses** and items to be seized listed in Attachments B-1 and B-2.

4. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook and Instagram to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

AFFIANT BACKGROUND

5. I have been a duly sworn law enforcement officer of the Baltimore Police Department since October 2001, authorized by and described under the Annotated Code of Maryland, Title 2, Subtitle 1, § 2-102, and am currently assigned to the Citywide Robbery Unit. I am also duly deputized by the United States Marshall. I have successfully completed a six-month

basic course of training that included classes pertaining to Policing, Law Enforcement, and Controlled Dangerous Substance violations.

6. My prior assignments include uniformed patrol, plain clothes narcotic enforcement, burglary investigations, non-fatal shooting investigations, robbery investigations, both physical and sexual child abuse investigations, and most recently commercial robbery investigations / Hobbs Act violations. I am also a Task Force Officer with the FBI, Violent Crimes Task Force, where I have personally conducted and participated in numerous investigations involving criminal activity in the aforementioned offenses including but not limited to Controlled Dangerous Substance violations, violent crimes, and firearms violations. I have also participated in hundreds of surveillances of persons who have violated the aforementioned crimes which has led me to participate in the arrest of numerous persons for the aforementioned violations. Subsequently, I have authored and/or executed more than 200 Search and Seizure Warrants relating to these crimes.

7. Through training as well as interviews and interrogations of hundreds of persons arrested for the above offenses, I am familiar with the actions, traits, and habits of persons who have committed these offenses specifically in the area of robbery. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and police officers, witnesses, police records, and reports.

8. In addition to the information described below, I submit that a search of the **Target Accounts** will reveal criminal evidence in the form of contact lists, private messages, posts, photographs, location information, and other media.

a. First, I know from training and experience that violent offenders who conspire to commit armed robberies, such as DINGLE, not only associate with one

another by cellular telephones, but also through social media accounts. Obtaining the contact lists (i.e. "Friend List") for the **Target Accounts** will help investigators understand DINGLE's conspiratorial network. Learning who these individuals associate with on social media will therefore clarify the scope of his conspiracy and also, more importantly, help identify members of the conspiracy that investigators do not, at this time, know. Also, I know that co-conspirators who commit armed robberies often have contacts, messages, and/or posts with one another.

b. Second, I know from training and experience that Facebook, Instagram, and other social media accounts are often helpful to ascertain what phone number a target is using and where they are located. For individuals who do not have each other's phone number, a social media account is the easiest way to find and contact someone. Similarly, a search warrant on a Facebook or Instagram account can reveal valuable contact and location information by understanding the times and places when a user accesses their account using a mobile telephone. A search warrant on Facebook and Instagram will allow investigators to identify the "IP Address" that accesses a particular account, at which point an investigator can subpoena the telephone provider of that IP Address to ascertain the phone number.

c. Third, I know from training and experience that violent offenders often post evidence of their criminal activity—e.g. photographs of U.S. currency, references to violence acts, and pictures of firearms and/or vehicles—on their social media accounts. However, the vast majority of such posts go to friends that are not publicly available on these accounts and which could reveal evidence of crimes. Because the vast majority of such posts, messages, and media content is "private," I cannot cite specific posts from the

Target Accounts in which DINGLE discusses robberies, contacts co-conspirators, or otherwise posts information about his location or activities.

d. Fourth, I know that Facebook often stores e-mail addresses, phone numbers, and other manners of communication of its users. As explained elsewhere, identification of the phone numbers and email addresses used by the targets of this investigation can lead to further evidence of the **Target Offenses** through comprehensive analysis of phone contacts, subscribers, and cellular location. Occasionally, as explained below, criminals will use Facebook itself as mode of communication to plan, conspire, and otherwise discuss criminal activities.

9. Because the content of the **Target Accounts** will remain preserved unless the user deletes such content, I submit that a search of these accounts will yield evidence of a crime inasmuch as those accounts will contain evidence from at or around the events summarized above.

10. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a search and seizure warrant, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, police officers, witnesses, cooperating sources, telephone records, and reports. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

11. With the assistance of the Baltimore Police Department, the Baltimore County Police Department, and the Anne Arundel County Police Department, the FBI is currently investigating a trend of armed Hobbs Act robberies that have occurred throughout Baltimore City, Baltimore County, and Anne Arundel County. The investigation encompasses robberies of the following stores:

• 4/09/2018	Spencer's One Stop Liquors	4300 Richie Highway
• 4/16/2018	Carney Liquors	9222 Harford Road
• 4/19/2018	Lucky's Superette	4225 Annapolis Road
• 4/24/2018	JP Liquors	6736 Richie Highway
• 5/12/2018	Subway	5520 Reisterstown Rd
• 5/22/2018	Nursery Liquors	6 Nursery Road
• 6/04/2018	Selma's Liquors	4600 Washington Blvd.
• 6/06/2018	Ridgeway Liquors	608 Edmondson Avenue
• 6/08/2018	Perry Hall Liquors	8673 Belair Road
• 6/21/2018	Euro Liquors	10512 Reisterstown Road
• 7/05/2018	5th Avenue Liquors	508 Crain Highway
• 7/12/2018	One-Stop Liquors	11700 Reisterstown Road

12. Some of the robberies involved multiple armed suspects; however, the primary suspect was as a black male, approximately 6'00", 200 pounds. During the robberies, he was armed with a silver handgun and typically forced the employees to the rear of the store at the conclusion of the robberies.

13. The suspect typically wore a disguise consisting of a costume, wigs, and glasses, as shown in the images below. For example, on June 21, 2018, during the robbery of Euro Liquors, the suspect was wearing a brown wig, wire framed glasses, a police costume shirt with the word "COP" written in white lettering on the front upper left portion of the shirt, a fake mustache, a white bandage on his right forearm (believed to hide a tattoo(s)), black pants, and black shoes. On July 5, 2018, during the robbery of 5th Avenue Liquors, the suspect was

wearing a wig, beard, red baseball hat, sunglasses, and a blue work shirt with stripes displaying the name "Michael" across the chest. On July 12, 2018, during the robbery of One-Stop Liquor Store, the suspect was wearing a dark colored fishing style hat, a green reflective construction jacket, an eye patch, a fake mustache, black pants, and black shoes.

14. While investigating the armed robbery of the One-Stop Liquor Store, investigators learned the suspect brought a bag of Dorito chips to the counter prior to the robbery, and then left the bag on the counter. The bag was processed for latent fingerprints. A latent fingerprint was recovered and submitted to the Baltimore County Police Department's Forensic Services Division- Latent Fingerprint Unit for analysis. The latent fingerprint was positively identified to be the left thumb of Donte Lamont DINGLE.

15. Investigators completed a criminal record check in regard to DINGLE, which revealed DINGLE has previous arrests and convictions for armed robbery. His date of birth is 07/08/1973, and his FBI number ends in 3PA2. DINGLE's physical description is listed as 5'11" and 196 pounds, which is similar to the video footage observed of the suspect in the above listed robberies.

16. Additionally, the suspect has been observed entering the front passenger-side of two "get-away vehicles" during the course of this trend:

- 2001-2003 Hyundai Elantra, gold/tan in color
- 1999-2001 Nissan Altima, gold/tan in color

17. During the investigation of the Euro Liquors robbery (occurred on June 21, 2018), video surveillance footage captured the suspect entering a Nissan Altima missing a rear license plate. Although the license plate was missing, the footage also captured a partially obscured license plate resting inside the vehicle on the rear seat. That license plate appeared to bear

Maryland Registration 8CT0799.

18. Two days after the robbery on July 12, 2018 of the One-Stop Liquors, Sergeant Rupp, of the Baltimore County Police Department, Towson Precinct, observed a gold 2000 Nissan Altima, bearing Maryland Registration 8CT0799 parked on the Days Inn parking lot, located at 8712 Loch Raven Blvd., Towson, Maryland, 21286. Sergeant Rupp recognized the vehicle to be similar to the Nissan Altima used by the suspects during the June 21, 2018 and July 12, 2018 robberies. A traffic stop was conducted on the vehicle as it left the Days Inn. The driver/owner was identified as Chardonnay Rachelle Cary, and the passenger identified himself as Demetrick Antoine Smallwood. Investigators later learned that both of these individuals are connected to Donte DINGLE.

19. Specifically, during the investigation, Detective Blevins with the Baltimore County Police Department examined the historical cell phone records for DINGLE, phone number 667-325-6521, and identified three outgoing telephone calls and one incoming telephone call regarding telephone number, 410-306-5118, which investigators learned is associated with Demetrick Smallwood, the passenger from the aforementioned traffic stop. Furthermore, a criminal record check for Smallwood revealed he has a prior robbery conviction in 2004. Further review of Donte DINGLE's historical cell phone records revealed multiple telephone calls between DINGLE's cellular phone, 667-352-6521, and cellular telephone number 443-922-1989, which is associated with Chardonnay Cary, the driver and owner of the 2000 Nissan Altima mentioned previously.

20. Beginning on July 17, 2018, investigators conducted surveillance on DINGLE. During the surveillance detail, investigators observed DINGLE exit and return to 5229 Saint Charles Avenue, Baltimore, Maryland 21215. Furthermore, investigators observed DINGLE

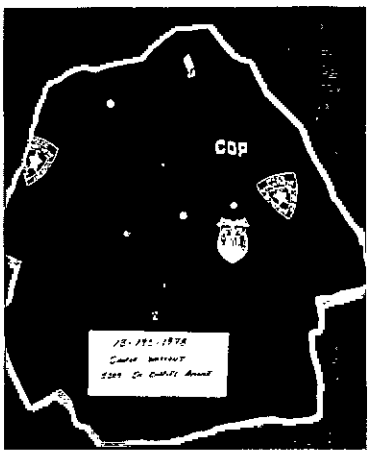
enter the address on the evening of July 18, 2018. Investigators believe DINGLE stayed the night. He then was observed exiting from that address on July 19, 2018.

21. Based on the information above, law enforcements obtained warrants to search: (1) 509 Mosher Street, Baltimore, MD 21217 (Chardonnay Cary's residence); (2) 5229 Saint Charles Avenue, Baltimore, MD 21215 (Dante DINGLE's residence); (3) a black 2006 Hyundai with Maryland registration 6DE0064 (Dante DINGLE's vehicle); and (4) a gold 2000 Nissan Altima, Bearing Maryland Registration 8CT0799 (Chardonnay Cary's vehicle). These warrants were executed during the morning of July 20, 2018.

22. After entering the location at 5229 Saint Charles Avenue, DINGLE's residence, law enforcement spoke with Donna Michelle Roundtree, who confirmed that "Donte" lived at 5229 Saint Charles Avenue in the upstairs middle bedroom.

23. A search of DINGLE's bedroom revealed numerous articles of clothing, wigs, glasses, and other disguises, several of which matched items worn by the suspect during the robberies. For example, the images below display items worn by the suspect during the Euro Liquors and 5th Avenue Liquors, respectively, next to items seized from DINGLE's bedroom:

Euro Liquors

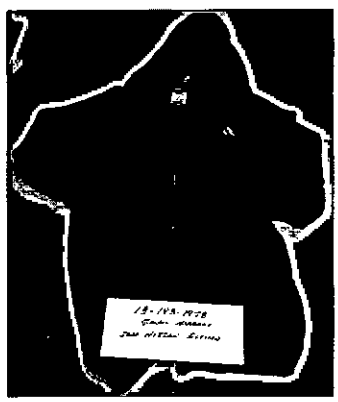


5th Avenue Liquors


24. In addition, law enforcement recovered from DINGLE's bedroom ammunition and a silver Bryco Arms Model T380 .380 caliber pistol, which appears to match the pistol brandished by the suspect during the robberies. Law enforcement also recovered $2,159.54 in U.S. currency.

25. That same day, around 8:15 am, law enforcement arrested DINGLE and transported him to 700 East Joppa Road, Baltimore County Police Headquarters.

26. Later that day, law enforcement also towed the gold Nissan Altimore to 700 East Joppa Road, Baltimore County Police Headquarters, and executed the search warrant of that vehicle. Inside the vehicle police found plastic disguise glasses and a black Adidas jacket with red trim matching the jacket worn by one of the suspects during the Carney Liquors robbery, as seen below:

27. On January 22, 2019, investigators with the FBI informed me that DINGLE appears to use the **Target Accounts** and that preservation requests had been served pursuant to 18 U.S.C. § 2703(f) requiring Facebook and Instagram to preserve all information associated with the **Target Accounts**. Investigators were able to identify the Facebook and Instagram accounts belonging to DINGLE by searching for usernames associated with DINGLE's name and aliases and by comparing the account user's viewable pictures on the social media accounts to known arrest pictures of DINGLE.

28. Given the facts set forth above, I submit that probable cause exists to believe that the **Target Accounts** contain evidence, fruits, and instrumentalities of the **Target Offenses**.

FACEBOOK

29. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

30. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

31. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual

Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

32. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

33. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

34. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

35. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

36. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

37. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

38. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

39. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

40. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

41. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

42. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

43. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like

Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

44. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account

activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INSTAGRAM

46. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram.

47. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at http://www.instagram.com. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

48. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various "tags" that can be used to search for the photo (e.g., a

user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of "filters" or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

49. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

50. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

51. Instagram allows users to have "friends," which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

52. Instagram also allows users to "follow" another user, which means that they receive updates about posts made by the other user. Users may also "unfollow" users, that is, stop following them or block the, which prevents the blocked user from following that user.

53. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

54. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

55. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

56. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP) address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

57. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

58. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

59. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.

60. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

61. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user's account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under

investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Instagram "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

62. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to DINGLE's account, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

Information To Be Searched And Things To Be Seized

63. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A), by using the warrant to require Facebook and Instagram to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B-1 and B-2. Upon receipt of the information described in Section I of Attachment B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachment B-1 and B-2.

CONCLUSION

64. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violations, of Hobbs Act robbery and conspiracy to commit Hobbs Act robbery (18 U.S.C. § 1951), felon in possession of a firearm (18 U.S.C. § 922(g)), and use of a firearm in furtherance of a crime of violence (18 U.S.C. § 924(c)) may be located in the **Target Accounts** described in Attachment A-1 and A-2.

65. Based on the forgoing, I request that the Court issue the proposed search warrant.

66. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

67. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Instagram and Facebook, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

19-0329 BPG 19-0330 BPG

Mohammed Ali
Task Force Officer, FBI

Sworn to before me this 25th day of January 2019

The Honorable Beth P. Gesner
United States Magistrate Judge

19 - 0329 BPG

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information associated with the following Facebook account:

Target Accounts	Profile Username	Numeric ID	Profile URL
Donte DINGLE a/k/a Donte Kane	Donte Kane	100007075992885	https://www.facebook.com/donte.kane

that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

19 - 0 3 2 9 BPG

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A-1:

(a) All contact and personal identifying information associated for each user ID identified on Attachment A-1, including the full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities from January 1, 2018 to July 20, 2018;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from January 1, 2018 to July 20, 2018, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which

the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the user from January 1, 2018 to July 20, 2018, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account from January 1, 2018 to July 20, 2018;

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of Hobbs Act robbery and conspiracy to commit Hobbs Act Robbery in violation of 18 U.S.C. § 1951, felon in possession of a firearm in violation of 18 U.S.C. § 922(g), and use of a firearm in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c), involving Donte DINGLE a/k/a Donte Kane since January 1, 2018, including, for each user ID identified on Attachment A-1, information pertaining to the following matters:

(a) All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes and steps taken to conceal these crimes;

(b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and

events relating to the crime under investigation and to the Facebook account owner;

(c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation.

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the target account and use of any robbery proceeds.

(f) The identity of the person(s) who communicated with the user ID about matters relating to offenses under investigation, including records that help reveal their whereabouts.

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel should make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

19-0330 BPG

ATTACHMENT A-2

Property to Be Searched

This warrant applies to information associated with the following Instagram account:

Target Accounts	Profile Username	Numeric ID	Profile URL
Donte DINGLE a/k/a Done Kane	Donte Kane666	1203080249	https://www.instagram.com/dontekane/

that is stored at premises owned, maintained, controlled, or operated by Instagram, LLC, a company that is owned by Facebook, Inc. and headquartered in Menlo Park, California.

ATTACHMENT B-2

19 - 0330 BPG

Particular Things to be Seized

I. Information to be disclosed by Instagram, LLC

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Instagram, LLC, including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, LLC, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Instagram, LLC is required to disclose the following information to the government for each account listed in Attachment A-1:

(r) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;

(s) All past and current usernames associated with the account;

(t) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(u) All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;

(v) All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

(w) All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

(x) All communications or other messages sent or received by the account from January 1, 2018 to July 20, 2018;

(y) All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content from January 1, 2018 to July 20, 2018;

(z) All photographs and images in the user gallery for the account from January 1, 2018 to July 20, 2018;

(aa) All location data associated with the account, including geotags from January 1, 2018 to July 20, 2018;

(bb) All data and information that has been deleted by the user from January 1, 2018 to July 20, 2018;

(cc) A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user;

(dd) A list of all users that the account has "unfollowed" or blocked;

(ee) All privacy and account settings;

(ff) All records of Instagram searches performed by the account, including all past searches saved by the account from January 1, 2018 to July 20, 2018;

(gg) All information about connections between the account and third-party websites and applications; and,

(hh) All records pertaining to communications between Instagram, LLC and any person regarding the user or the user's Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of Hobbs Act robbery and conspiracy to commit Hobbs Act Robbery in violation of 18 U.S.C. § 1951, felon in possession of a firearm in violation of 18 U.S.C. § 922(g), and use of a firearm in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c), involving Donte DINGLE a/k/a Donte Kane since January 1, 2018, including, for each user ID identified on Attachment A-1, information pertaining to the following matters:

(a) All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes and steps taken to conceal these crimes;

(b) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and

events relating to the crime under investigation and to the Instagram account owner;

(c) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation.

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the target account and use of any robbery proceeds.

(f) The identity of the person(s) who communicated with the user ID about matters relating to offenses under investigation, including records that help reveal their whereabouts.

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel should make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.